A Developing Science of Cyber Security – an Opportunity for Model Based Engineering & Design

October 26, 2017

Jerry M. Couretas, PhD

About Me - Cyber Modeling and Simulation

- 2016 – presentOSD C3CB Cyber Mission Model and Economics of Cyberspace Performance Working Group Lead
- 2013 – 2016 Coordinated OSD DM&SCO Cyber M&S Technical Working group for
- Editor-in-Chief of the Journal of Defense Modeling and Simulation
  - 7/2017 Cyber M&S Special Issue
  - 1/2018 Cyber Special Issue on Developing Science of Cyber Security


GREENLAND
CANADA
RUSSIA
UNITED STATES
CHINA
MEXICO
BRAZIL
ARGENTINA

Hackers Are Targeting Nuclear Plants, U.S. Says

By NICOLE PERLROTH

Since May, hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries.

Among the companies targeted was the Wolf Creek Nuclear Operating Corporation, which runs a nuclear power plant near Burlington, Kan., according to security consultants and an urgent joint report issued by the Department of Homeland Security and the Federal Bureau of Investigation last week.

The joint report was obtained by The New York Times and confirmed by security specialists who have been responding to the attacks. It carried an urgent amber warning, the second-highest rating for the severity of the threat.

The report did not indicate whether the cyberattacks were an attempt at espionage — such as stealing industrial secrets — or part of a plan to cause destruction. There is no indication that hackers were able to jump from their victims' computers into the con-

DAVID EULITT/CAPITAL JOURNAL, VIA ASSOCIATED PR

The Wolf Creek nuclear plant in Kansas in 2000. Its operator was targeted by hackers.

cause of confidentiality agreements.

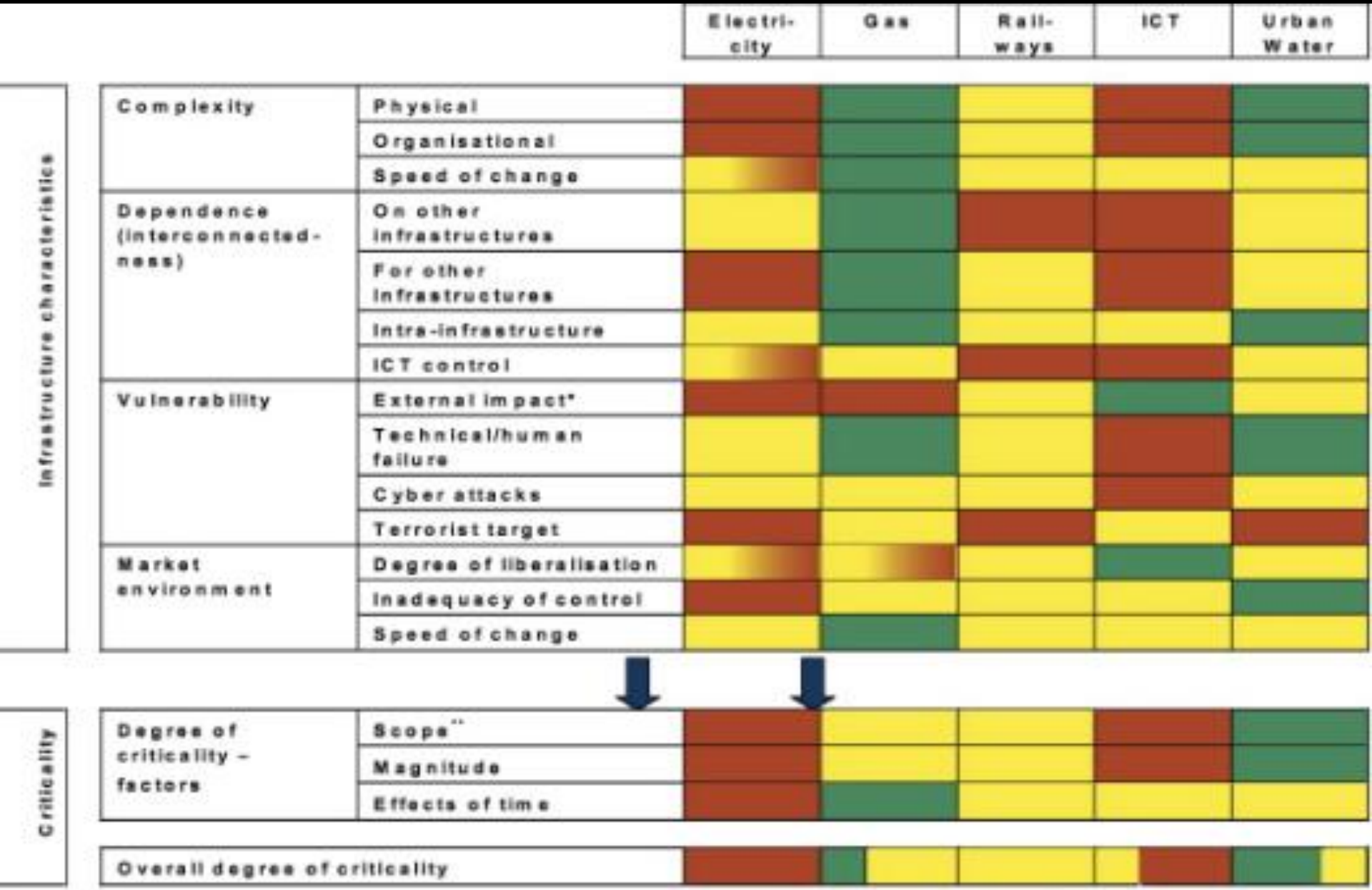
The origins of the hackers are not known. But the report indi-

directed their victims' internet traffic through their own machines.

Energy, nuclear and critical manufacturing organizations

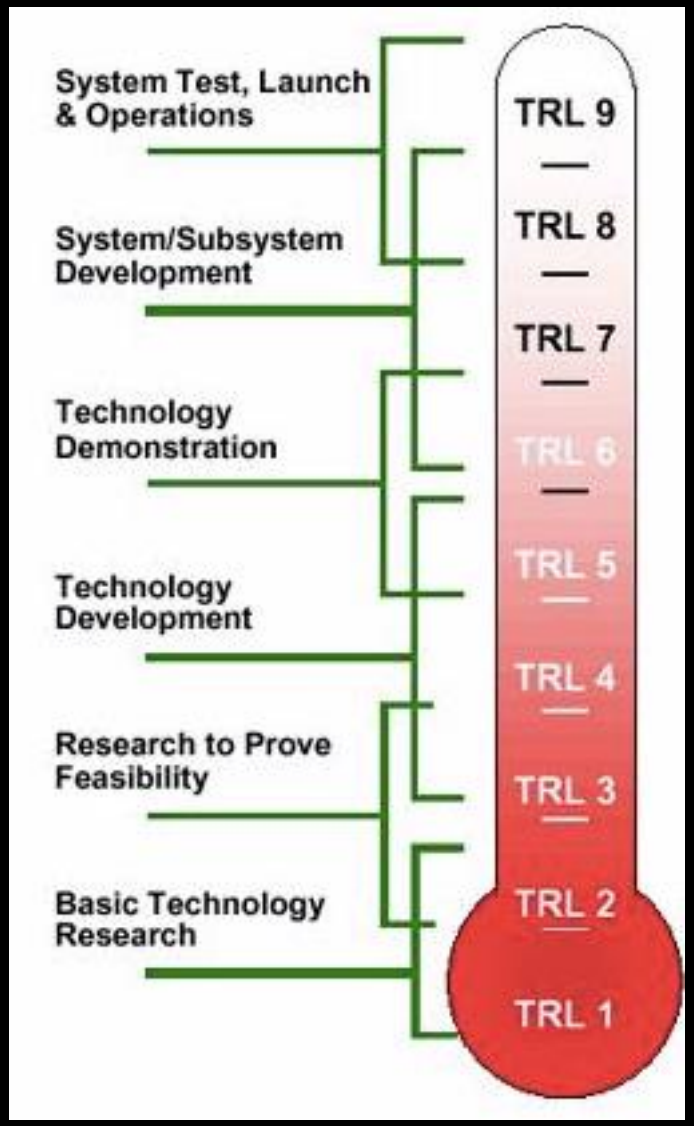
"We never anticipated that critical infrastructure control s tems would be facing advan levels of malware," Wellinghoff said.


DISASTER
CITY
TEEX


Electri-city
Gas
Rail-ways
ICT
Urban Water
Infrastructure characteristics
Complexity
Physical
Organisational
Speed of change
Dependence (interconnected-ness)
On other infrastructures
For other infrastructures
Intra-infrastructure
ICT control
Vulnerability
External impact*
Technical/human failure
Cyber attacks
Terrorist target
Market environment
Degree of liberalisation
Inadequacy of control
Speed of change
Criticality
Degree of criticality – factors
Scope**
Magnitude
Effects of time
Overall degree of criticality

Cyber in the News
(Stoplight Charts)

M&S Work



NASA Technological Readiness Levels (TRLs)

Contents

- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up

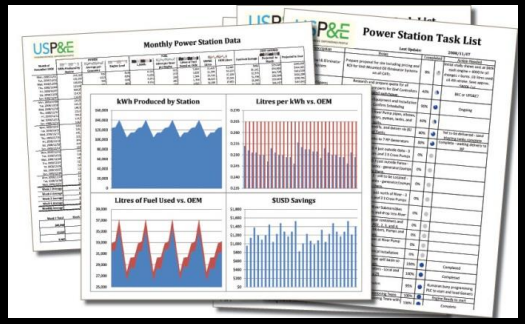
Contents

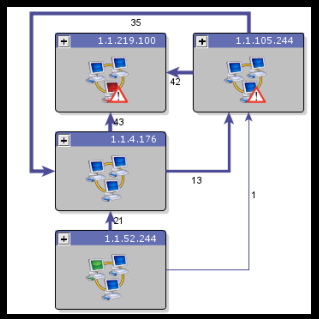
- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up

The Scientific Underpinnings of Cybersecurity[1]

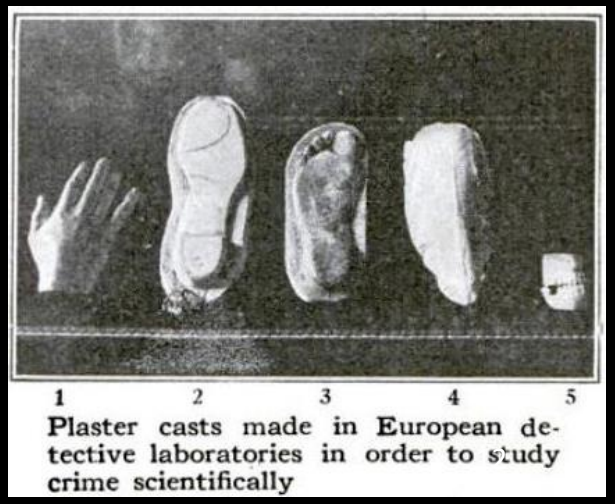
A science of security will develop

- a body of scientific laws
- testable explanations
- confirmation or validation of predicted outcomes





CyVision Network Layout


1 2 3 4 5
Plaster casts made in European detective laboratories in order to study crime scientifically

[1] https://mail.google.com/mail/u/0/#search/nas/15c758e80b12d023

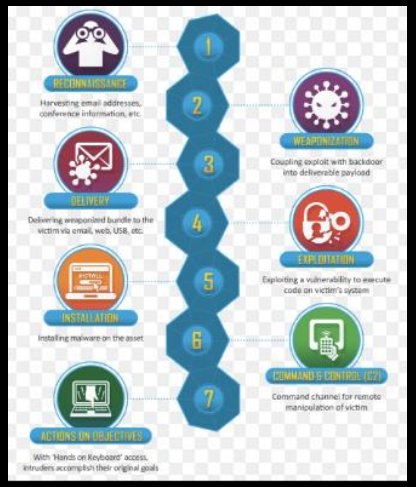
Scientific Approach to Cybersecurity

There are strong and well-developed bases in the contributing disciplines:

- mathematics and computer science
- human sciences[1]

A scientific approach to cybersecurity challenges expands understanding of

- systems
- defenses
- attacks
- adversaries



[1] https://www.amazon.com/Research-Methods-Cyber-Security-Thomas/dp/0128053496

National Academy of Science & Cyber Research

Findings included

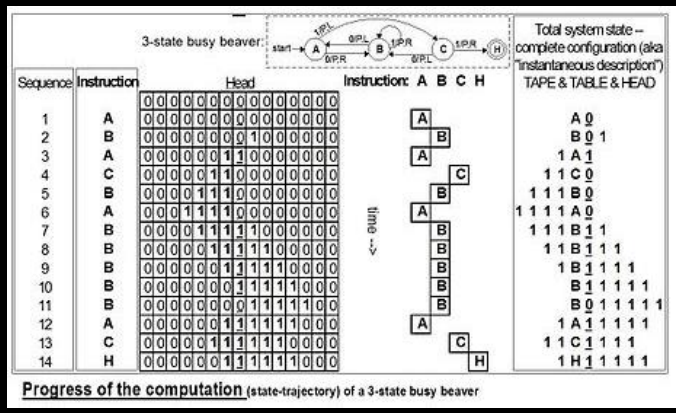
- Interdisciplinary program examples – U of Bochum
- Questions current research
  - High frequency publishing vs quality
  - Enabling results
- Longer research projects may help

[1] https://mail.google.com/mail/u/0/#search/nas/15c758e80b12d023

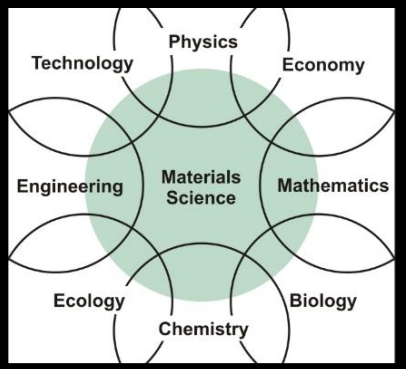
Example Transitions from Art to Science

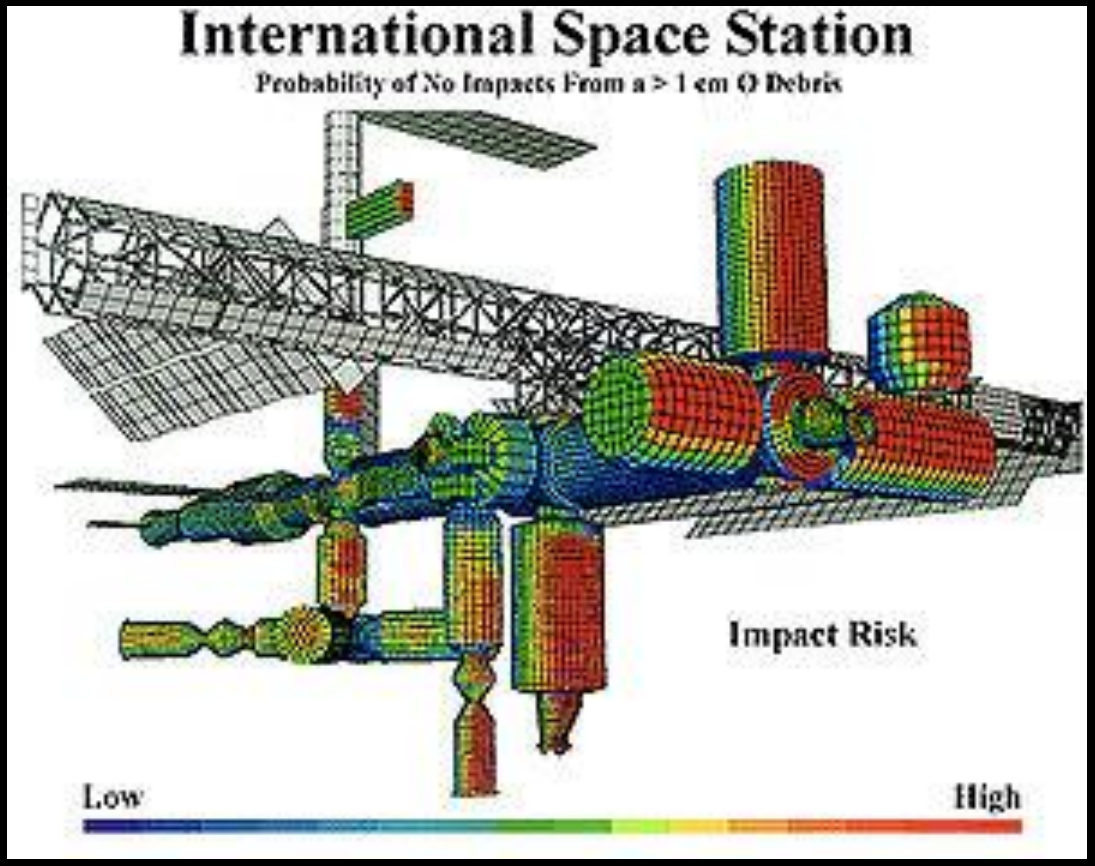
- ***Cyber Security Science***
  - 1700s– 1960s – complex industrial systems with integrated timing handled by respective operators
  - 1960s – 1980s – Systems Theory (e.g., Wymore, Zeigler …) texts introduced
  - 1990s – 2000s – micro computers increased number of entities to point where scale and scope of new systems introduce overall security / safety issues
  - Early 2000s – present – "cyber" introduced as topic in security circles
  - Next step ?

- Computer Science
  - Pre History – 1930s – "computer" was a person who used various devices (e.g., Abacus, analytical engine, etc.)
  - 1930s – 1950s – algorithms (e.g., Church-Turing, …), N. Wiener's "Cybernetics," identified as independent domain
  - 1950s – 1970s – development of computer science curricula and specialized literature (e.g., first PhD ~ 1965)
  - 1970s – present – "Computer Science" with provable hypotheses



- Material Science
  - Pre History to 17th Century – Alchemy
  - 17th Century – 1960s – Metallurgy
  - 1960s – present - Material Science
  - ➢ Still recipe based





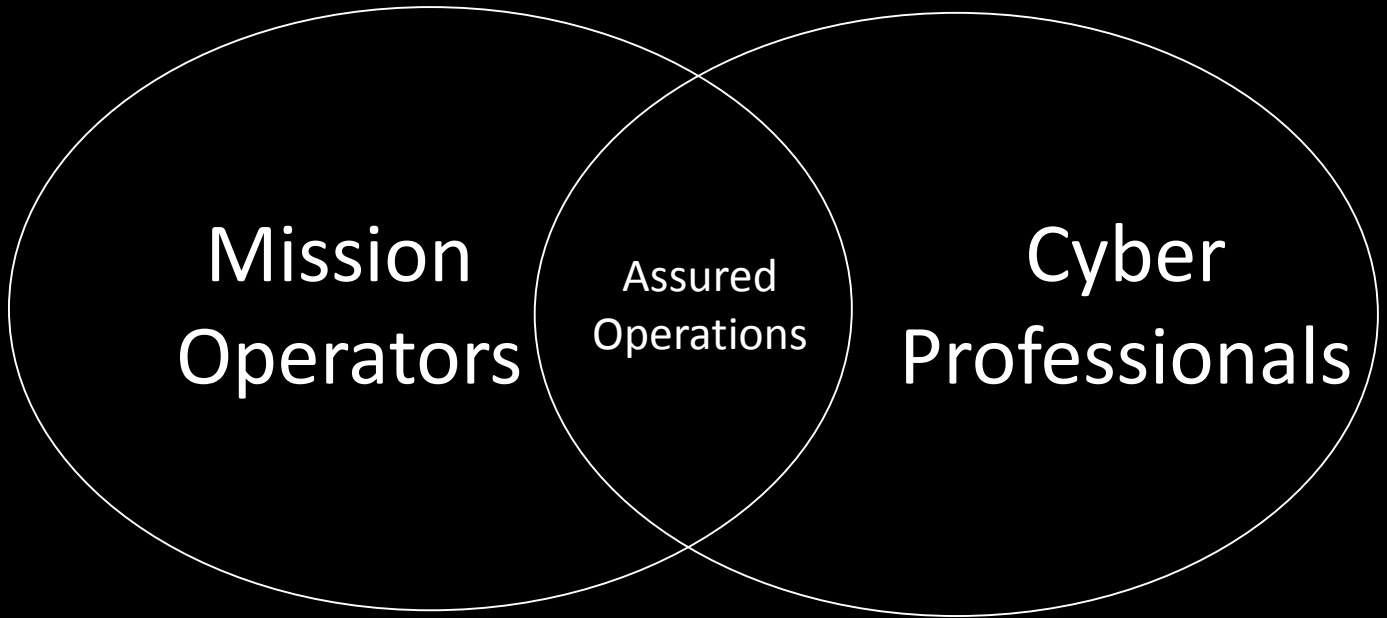
We have built high risk, complex systems, for new domains

Hard Problems are what M&S is For

Contents

- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up

Cyber Mission M&S Communities



Cyber for Others

Cyber for Cyber

Cyber for Others, C4O

- Recognise cyber attack indicators
- React – call C4C

Cyber for Cyber, C4C

- Block network attacks
- Mitigate network attacks
- Reconstitute networks

Military Activities & Cyber Effects (MACE)[1]

Military Effects(C4O)

Cyber Effects (C4C)

	Deny	Degrade	Disrupt	Destroy	Digital Espionage
Interruption	✓	✗	✓	✗	✗
Modification	✓	✓	✓	✓	✗
Degradation	✗	✓	✓	✗	✗
Fabrication	✓	✓	✗	✗	✓
Interception	✗	✗	✗	✗	✓

[1] Bernier, M. (2015). *Cyber Effects Categorization - The MACE Taxonomy.* DRDC Center for Operational Research and Analysis. TTCP JSA TP3 Cyber Analysis

Example Cyber Mission Use of Standards

- OASIS standards address IA to protect
  - CybOX (Cyber Observable eXpression)
  - STIX (Structured Threat Information eXpression)
  - TAXII (Trusted Automated eXchange of Indicator Information)

- *Cyber Range Interoperability Standard (CRIS) to connect different range emulations*[1]

  - SISO Training Standards

[1] http://www.dtic.mil/ndia/2014/test/Ferguson.pdf

Contents

- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up

2015 Business Blackout

Lloyd's of London scenario looked at a U.S. power grid failure

[1] https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout

… and, while a major cyber attack is unlikely …

Cyber attacks, including against industrial control systems, are a continuing phenomena

Date	Event name	Detailed description	Actors	Motivation	Methodology	Outcome
April 1999 (Milhorn, 2007)	**Gazprom – Russian gas supplier**	A Trojan was delivered to a company insider who opened it deliberately. The control system was under direct control of the attackers for a number of hours.	Targeted Attack & Insider	Sabotage & Ransom	Trojan & Insider	Unauthorised Access
July 1999 (National Safety Transport Board, 2002) (Wilshusen, 2007)	**Bellingham**	Over 250,000 gallons of gasoline leaked into nearby creeks and caught on fire. Large amount of property damage, three deaths and eight others injured. During the incident the control system was unresponsive and records/logs were missing from devices.	Accident	Unknown	Accidental	Physical Damage and Bodily Injury
Feb. and April 2000 (Jill Slay, 2008) (Wilshusen, 2007)	**Maroochyshire**	A recently fired employee sabotaged radio communications and released 800,000 gallons of raw sewage into parks, rivers and the grounds of a hotel.	Insider attack	Sabotage	Radio man-in-the-middle	Physical Damage
May 2001 (US House of Representatives, 2005 (SCADA)[1] Systems and the Terrorist Threat: Protecting the Nation's Critical Control Systems, 2005	**California**	A hacking incident at California Independent System Operator (CASO) lasted two weeks, but did not cause any damage.	External attack	Unknown and contained	Deliberate	Thwarted
August 2005 (GAO Report, 2007)	**Daimler Chrysler**	Thirteen Daimler-Chrysler US auto manufacturing plants were taken offline for about an hour by an internet worm. An estimated $14m in downtime costs.		Spyware Installation	Zotob Worm and MS05-039 Plug n-Play	Infection
Infection	**Brown's Ferry**	Loss of recirculation flow on a US nuclear reactor down for maintenance caused a manual scram. A worm exploited a buffer overflow flaw in the widely used MSSQL server during the scram.		Unknown	Slammer Worm and Buffer Overflow	Non-industrial control systems targets
Oct 2006 (Wilshusen, 2007)	**Harrisburg**	Hackers gained access to a water treatment plant through an infected laptop.	Targeted Threat Agent	Mischief	Compromised Laptop	Server used to run online games
Jan 2008 (Maras, 2012)	**Lodz**	Attacker built a remote control device to control trains and tracks through distributed field devices. Four trains were derailed with zero deaths. A disgruntled employee installed malicious code on a canal control system.	Targeted Threat Actor, Accident or Insider Attack	Mischief	Altered Universal Remote	Mayhem, Criminal Damage
Jan 2008 (Knapton, 2008)	**Kingsnorth**	Attacker broke into the E.ON Kingsnorth power station which caused a 500MW turbine to take an emergency shutdown.	Targeted Threat Actor	Sabotage	Physical Penetration	Environmental Project

Insurance Concepts & Systems Engineering for Cyber

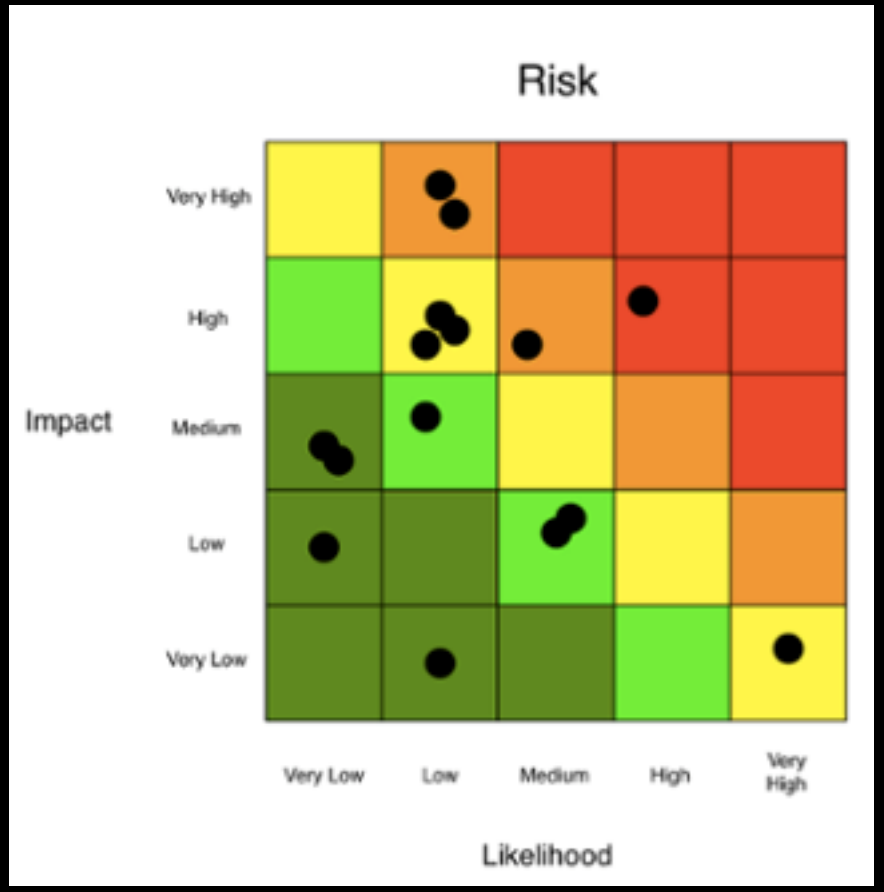
- Böhme & Schwartz (2010) provide an excellent summary of cyber insurance literature and define a unified model of cyber insurance that consists of 5 components:
  - the networked environment
  - demand side
  - supply side
  - information structure
  - organizational environment

- In addition, the defining characteristics of cyber insurance are
  - interdependent security
  - correlated failure
  - information asymmetry

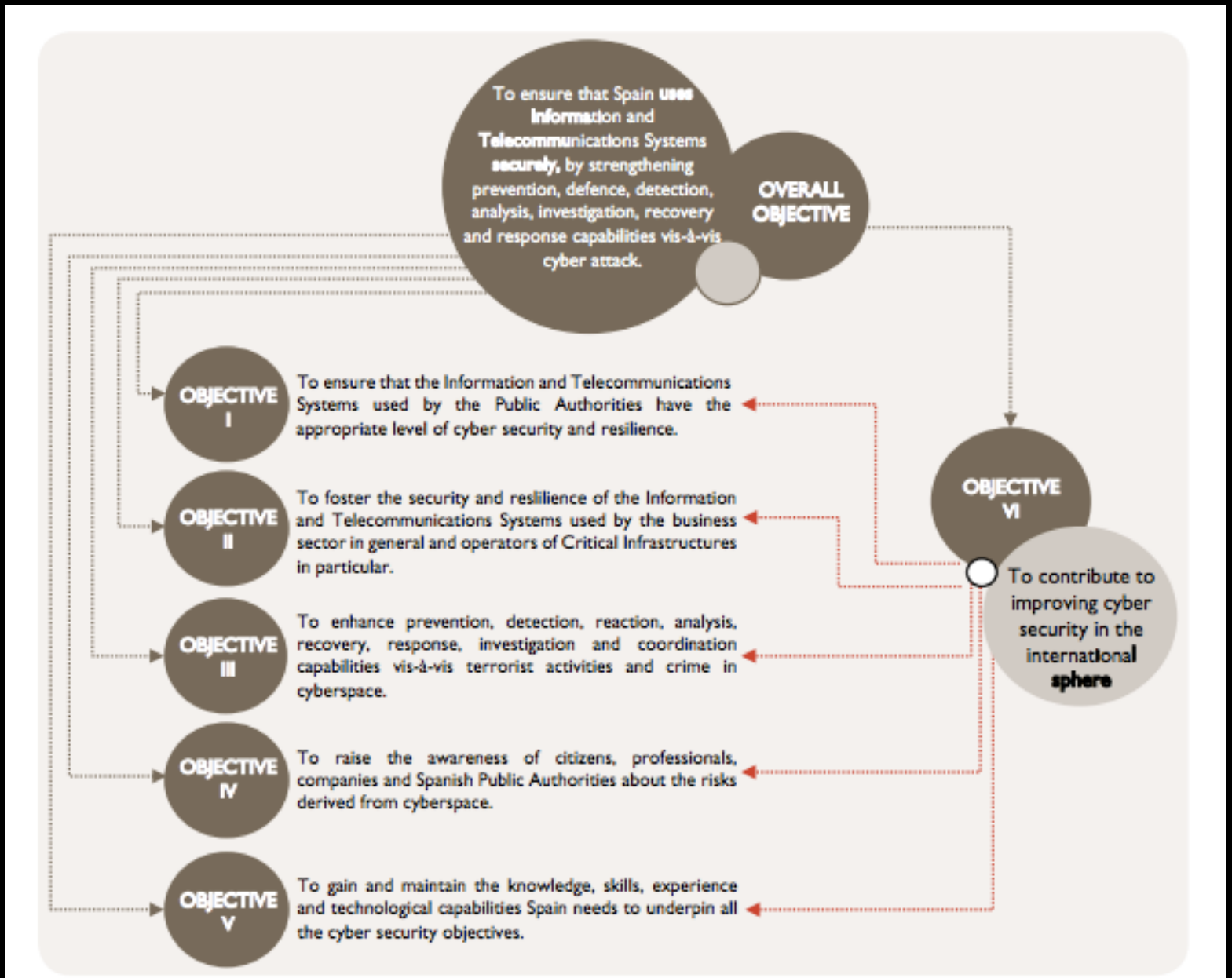
[1] http://mobile.royalgazette.com/business/article/20170714/ics-sees-ratings-as-key-for-cybersecurity&template=mobileart

Example Cyber Measurement Models

- Factor Analysis of Information Risk (FAIR) Model [1]
- "How to Measure Anything in Cyber Security Risk"[2]



1 http://www.fairinstitute.org/
2 http://www.howtomeasureanything.com/cybersecurity



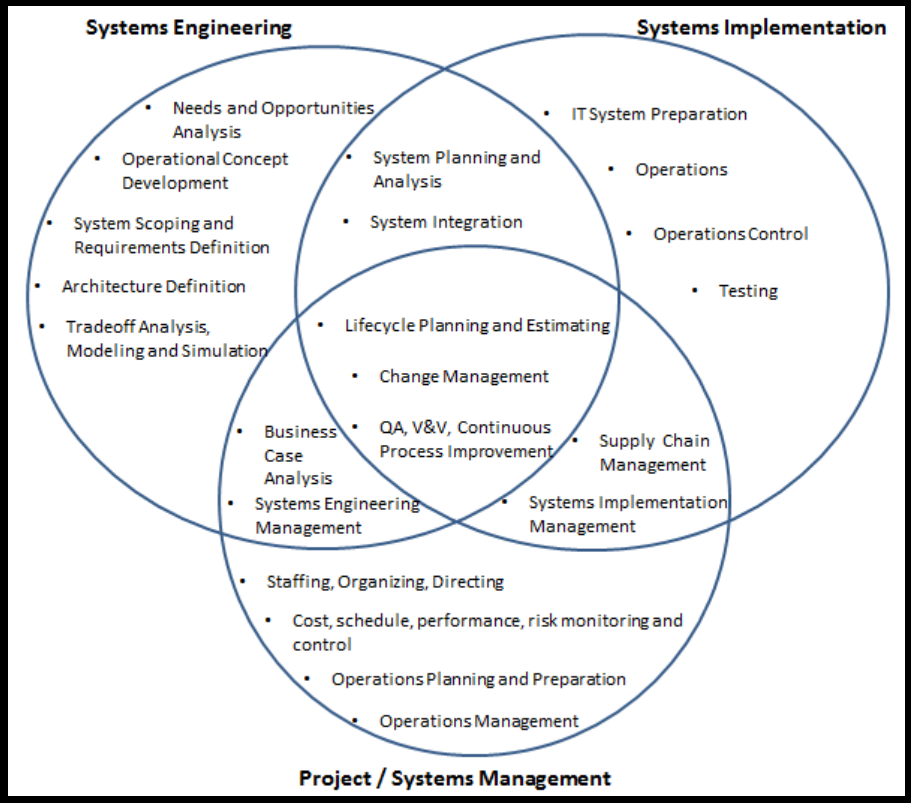
[1] https://www.enis

Contents

- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up

Cyber Model Example - Introduction

- Build Enterprise Description Model
- Use Analytic Model

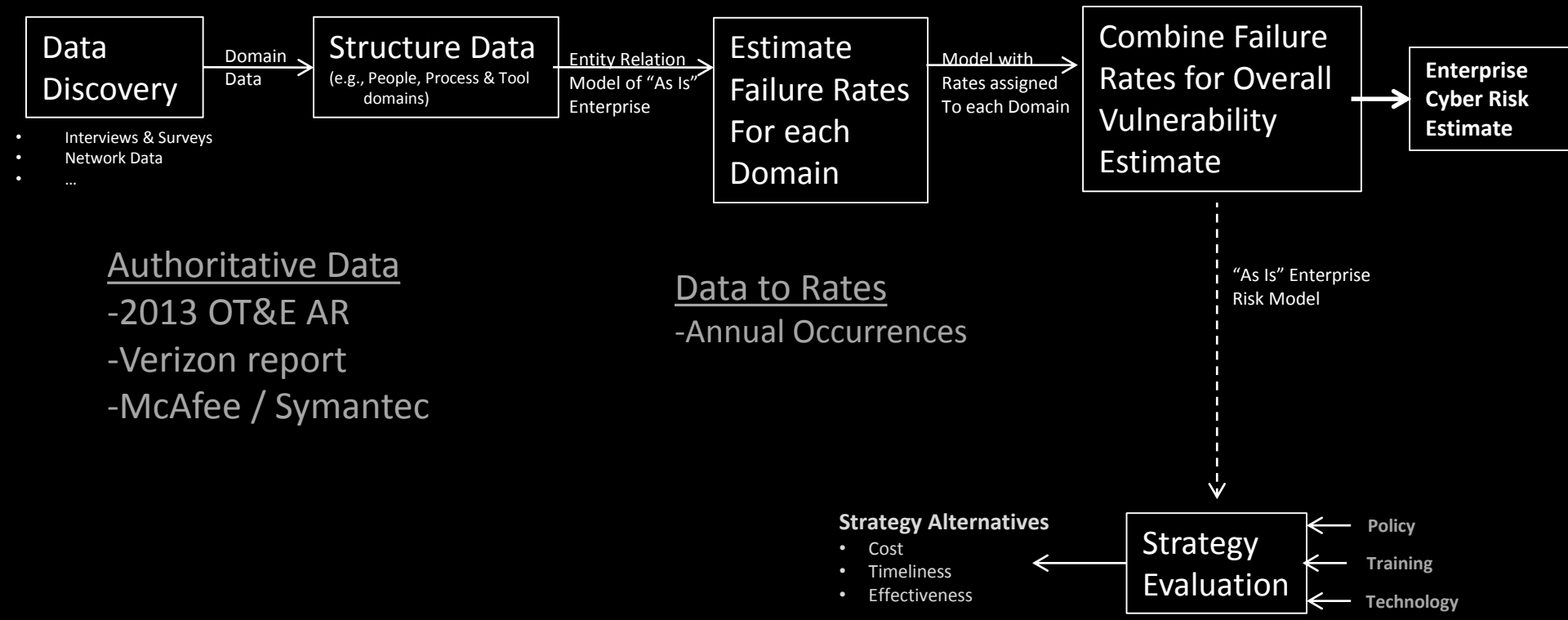


Enterprise Model

People manage enterprise due to the scope of information

[1] http://www.itl.nist.gov/div898/handbook/apr/section1/apr161.htm

Enterprise Model Construction & Evaluation



Authoritative Data
-2013 OT&E AR
-Verizon report
-McAfee / Symantec

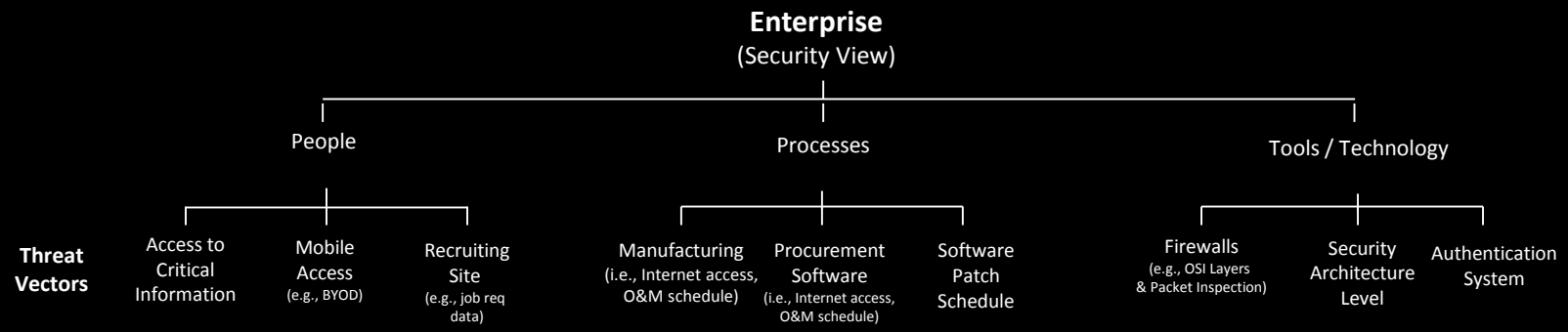
Data to Rates
-Annual Occurrences

Metrics
-Dollar quantifiable (e.g., Target, Nieman Marcus …)
-Media quantifiable (e.g., Snowden, Manning) – number of articles / exposure

Enterprise Model

(Populate with known Data)

People, Processes & Tools from Surveys / Interviews

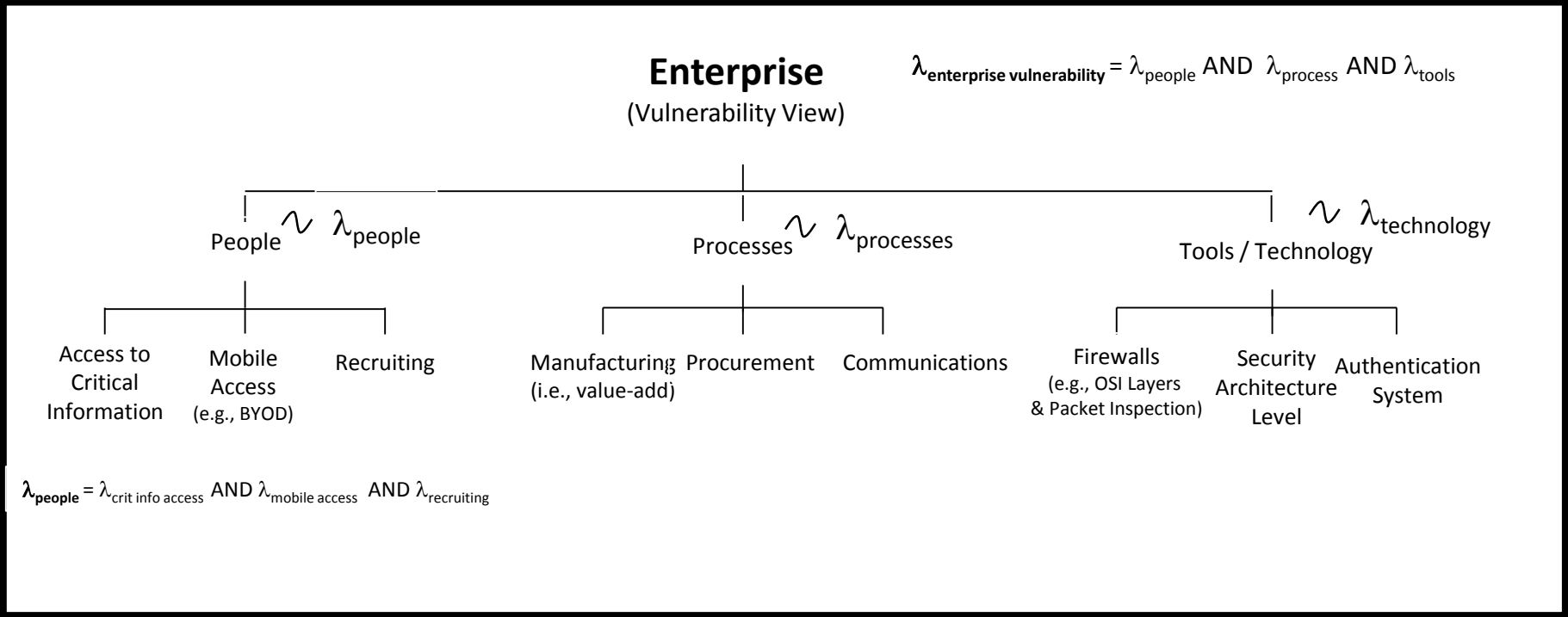


Q&A to Static Enterprise Model

Use the Q&A process to develop an information structure amenable to modeling:

	People	Processes	Tools
Who	• System Access		• User Authentication
What	• Personally Identifiable Information (PII) • Social Media	• Critical Information • High Volume (e.g., manufacturing)	
When	• System Access	• Maintenance Schedule • Patch Schedule • Software Updates	
Where	• Fixed Site • Mobile		
Why	• Business System access • Technology System Access		• Secure Sockets Layer (SSL)
How	• Recruiting • Screening		• Security Architecture Level • Firewall – monitoring & control

Enterprise Model & Parameterization
(organize respective failure rate estimates)

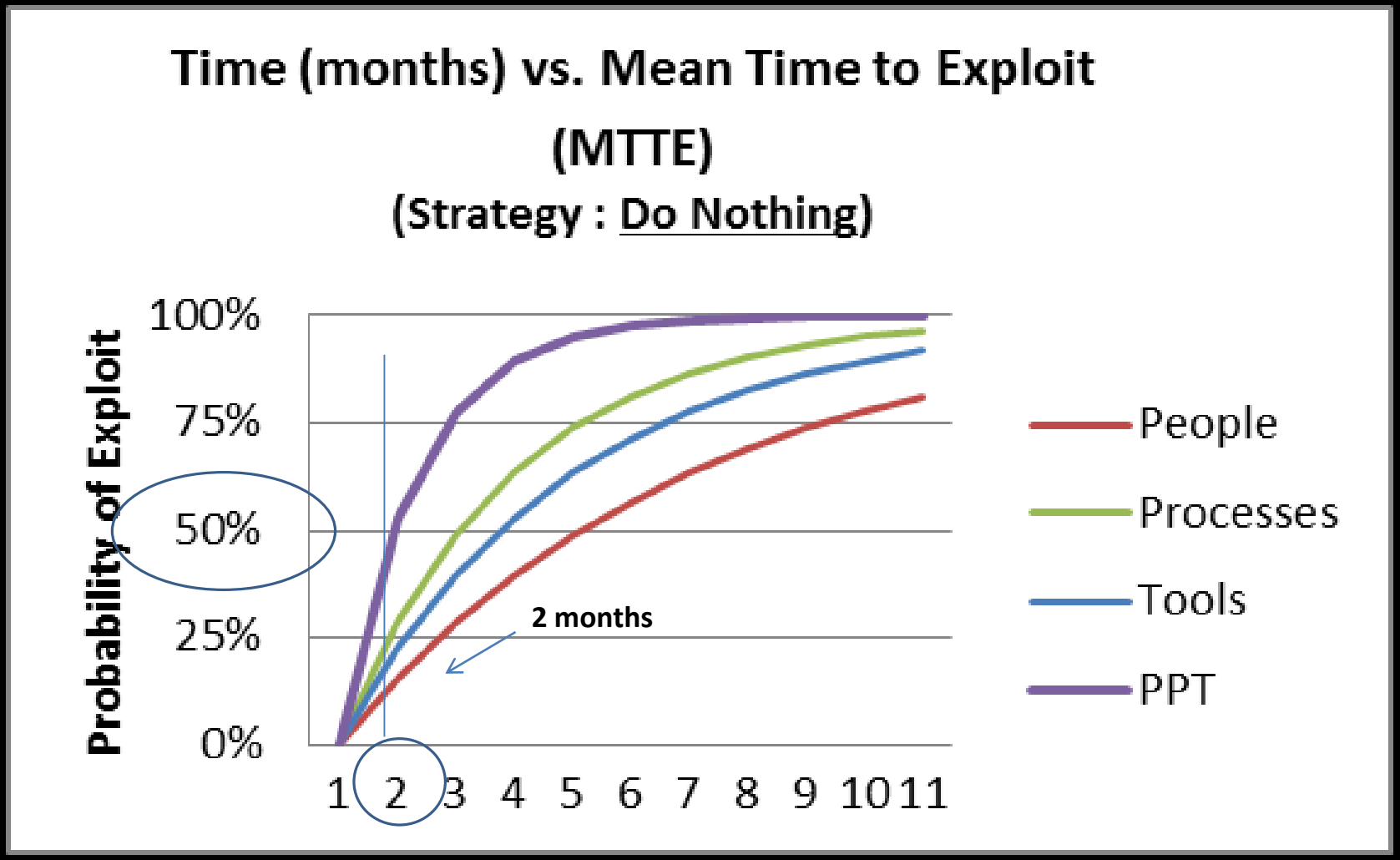


- λ is the failure rate for the respective domain (e.g., people, process, tool) or one of its components

- Exponential distribution results in “additive” combination of failure rates over the heterogeneous data for the respective domains

“As Is” Risk Estimation

(Strategy – “Do Nothing”)

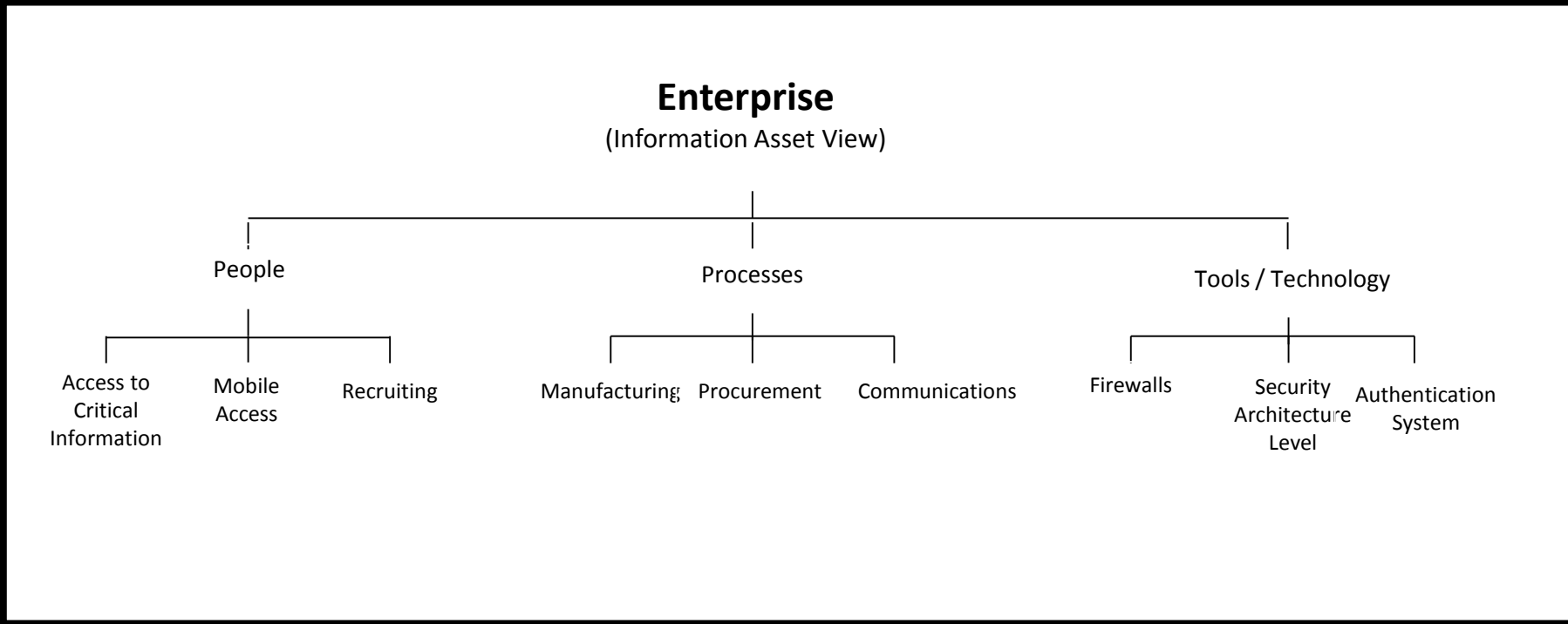


Example Countermeasures as Work Packages

Packages / Domain & Work Package		Cyber Enterprise Domain Affected by Work Packages			Work Package Time / Cost Estimate	
Work Packages		People (λ_{people})	Process ($\lambda_{process}$)	Tool (λ_{tool})	Implementation Time	Cost ($ K)
	Access	●	○	○	months	10's
Policy	Mobile Device	●	●	●	months	10's
	Critical Information	●	●	○	months	10's
	Phishing	●	○	○	weeks	10's
Training	Internet Use	●	○	○	weeks	10's
	Social Engineering	●	●	○	weeks	10's
	Firewalls	○	●	●	days	100's
Technology	M&C	○	○	●	days	100's
	Authentication	●	○	●	weeks	100's

- Work Packages provided as policy / training / technology "fixes" and affect cyber enterprise domains (i.e., people, processes and tools) independently
- Independent Work Package provision results in ready project plans in terms of time and cost estimates for improving enterprise resiliance

Model Based ⟺ Knowledge based



[1] "Artificial Intelligence and National Security" (http://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf)

Contents

- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up

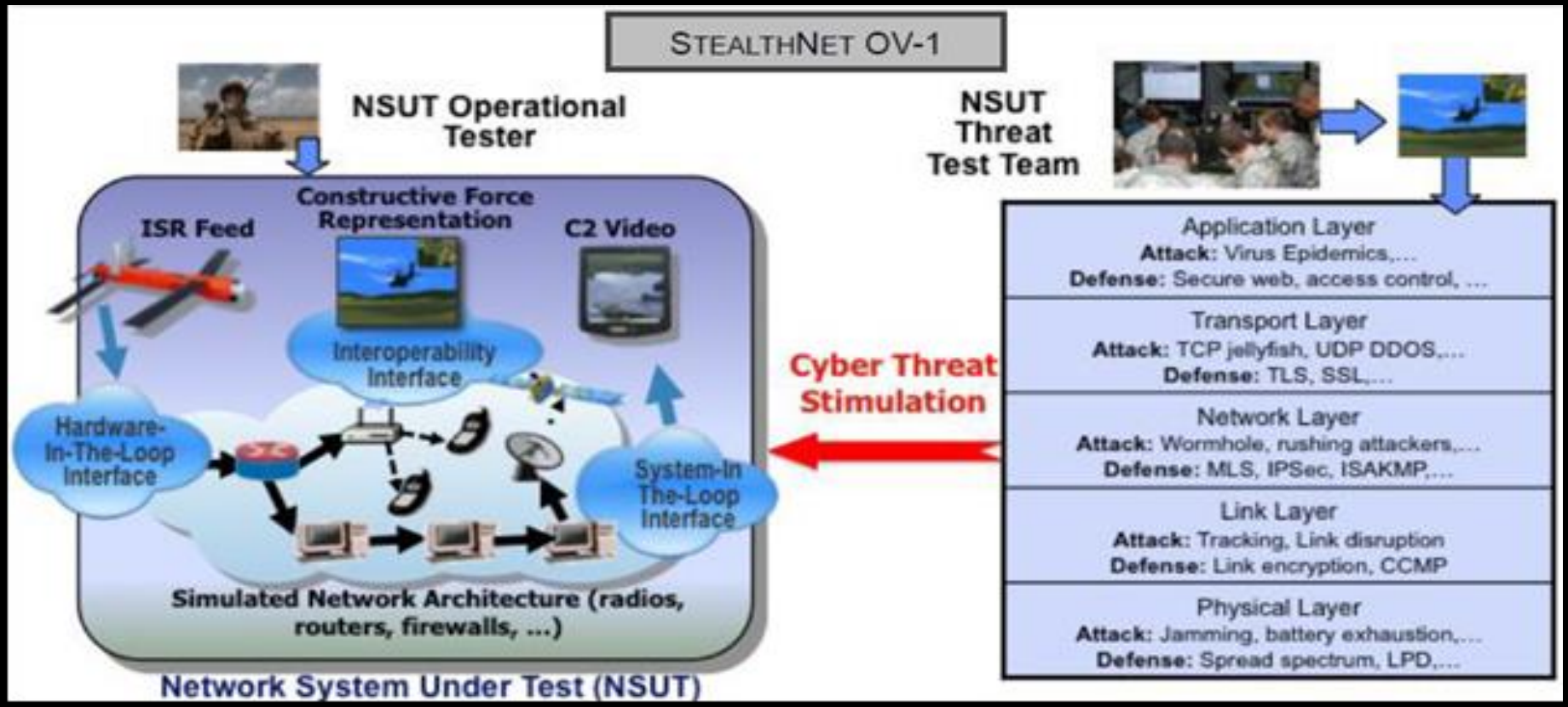
Nissan Quest / Ford Villager

- 7 Prototype builds
- 1000s of hours of testing / evaluation

Death Valley Hot Weather Testing

Bemidji MN Cold Weather Testing

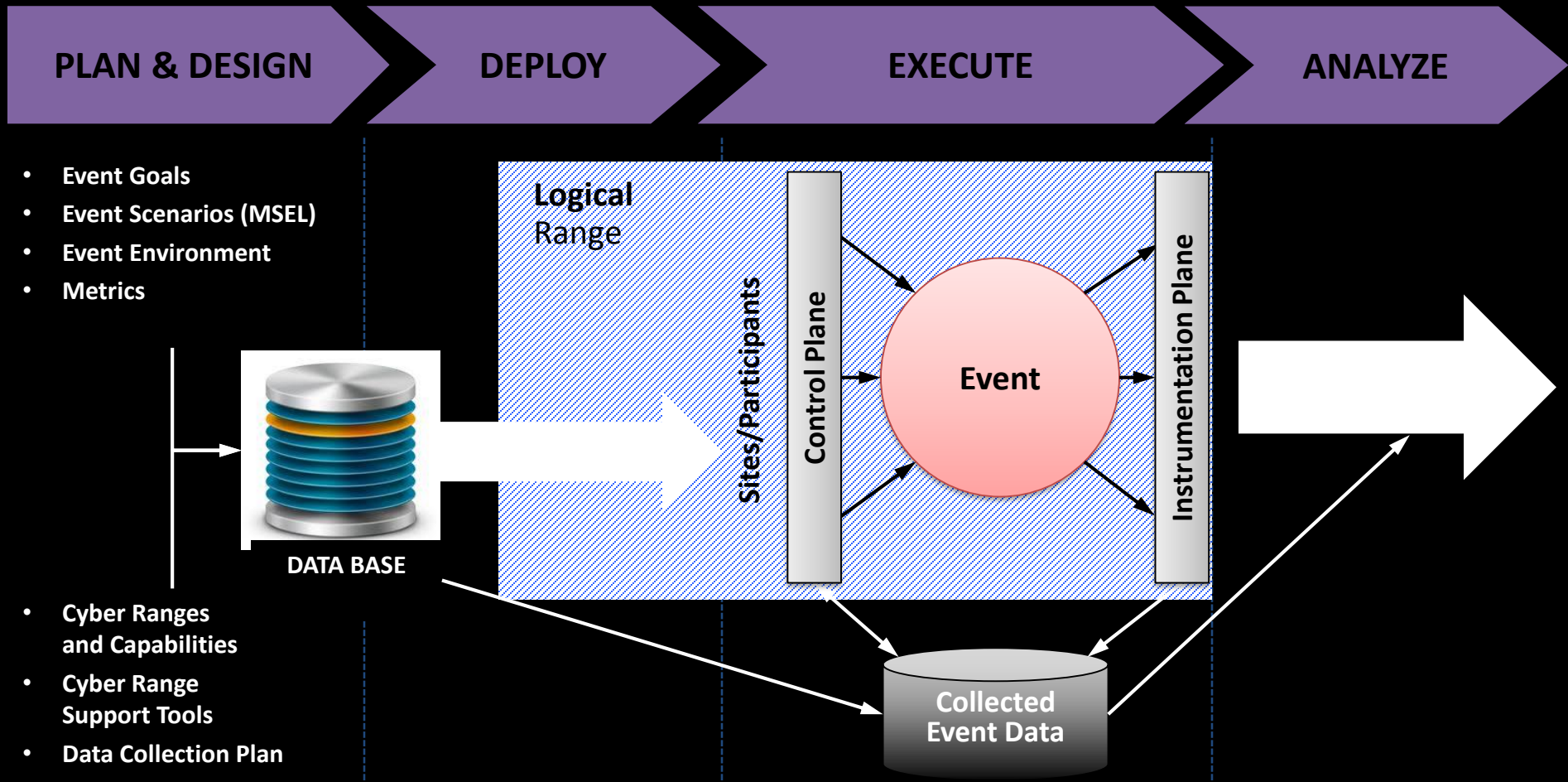
Cyber M&S / Test Example



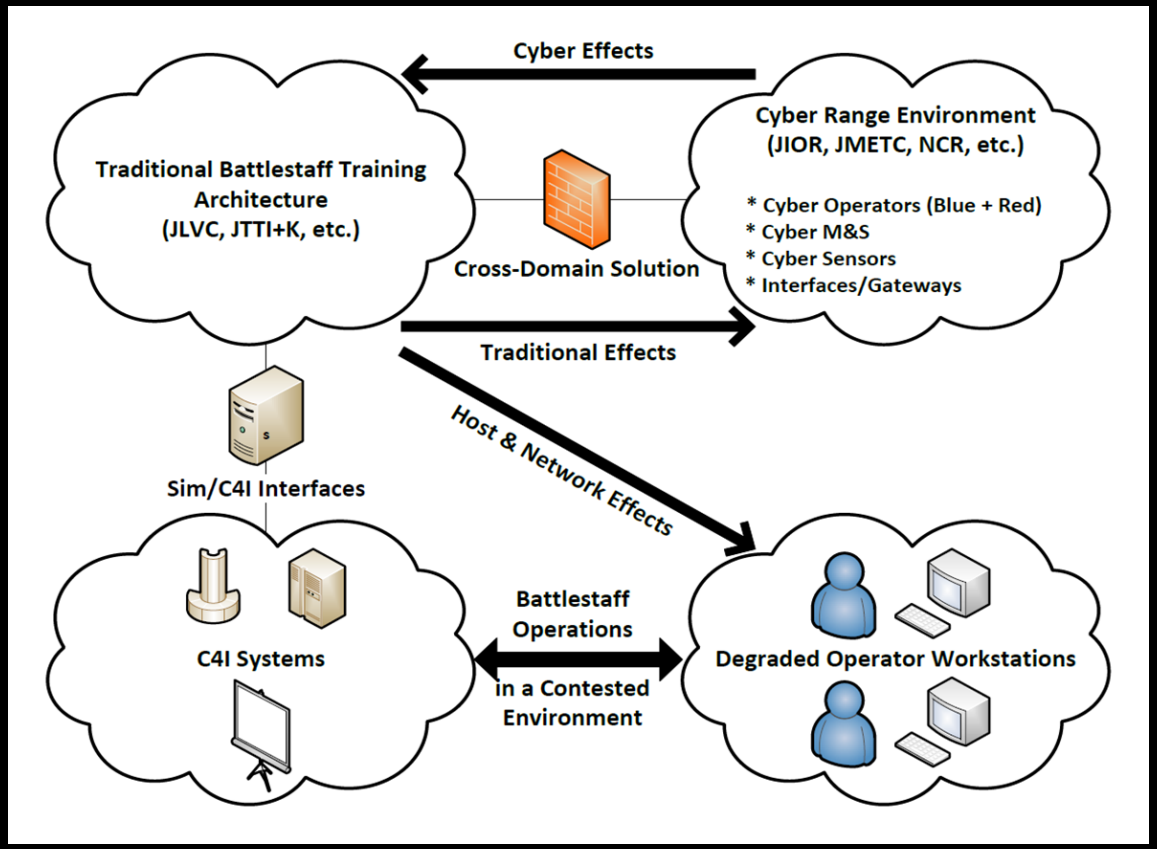
Network Emulation (StealthNet) injection into Network System Under Test (NSUT)[1]

[1] http://www.dtic.mil/ndia/2012/system/ttrack514951.pdf

Cyber-Range Event Process Overview



Cyber Operations Architecture Training System (COATS)[1]



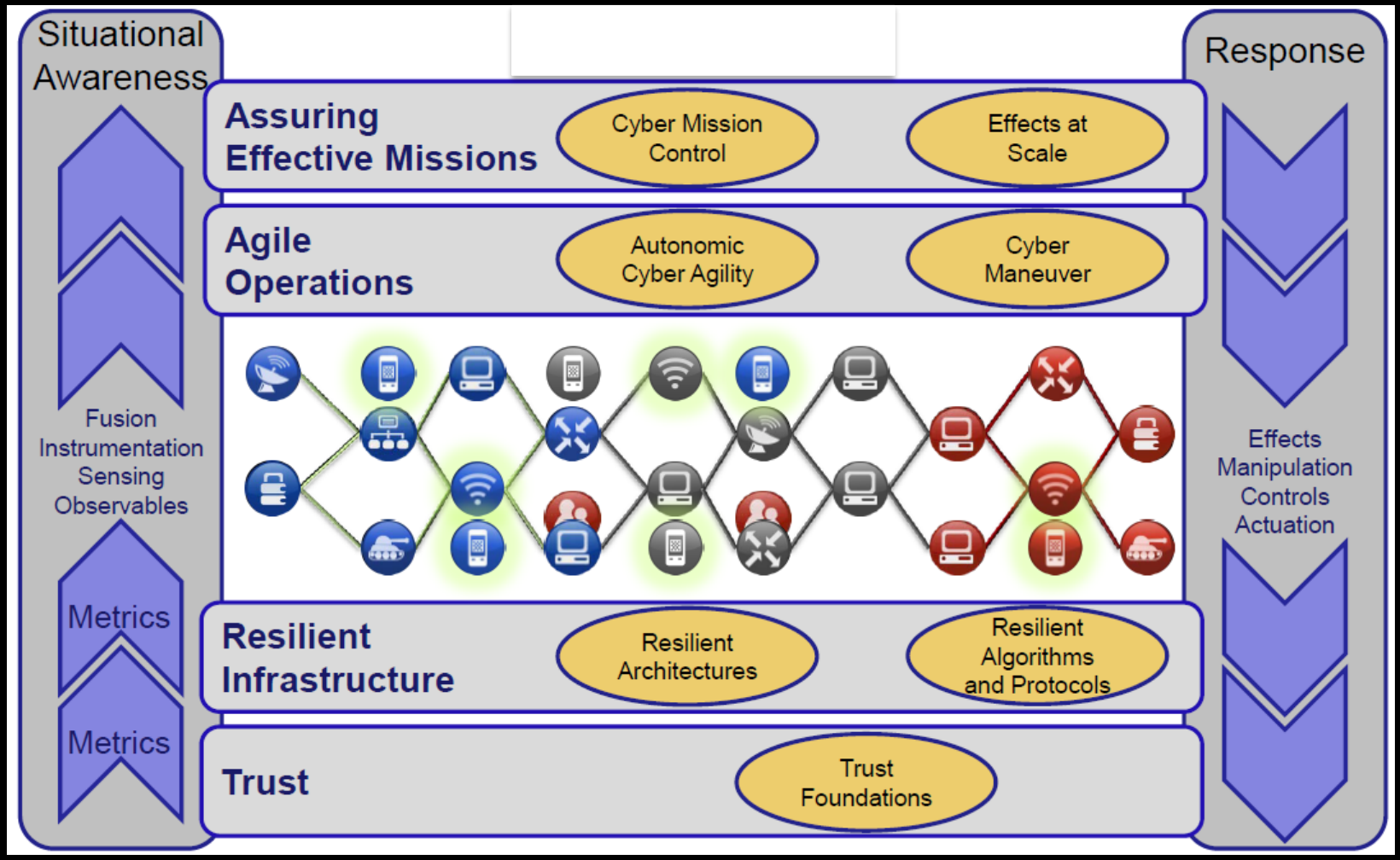
Inject Cyber Range effects into Command Staff training simulations

[1] 2015 I/ITSEC Best Paper (http://www.iitsec.org/about-iitsec/publications-and-proceedings/best-papers-and-tutorials-from-past-iitsec)

"I'm no expert, but I think it's some kind of cyber attack!"

Contents

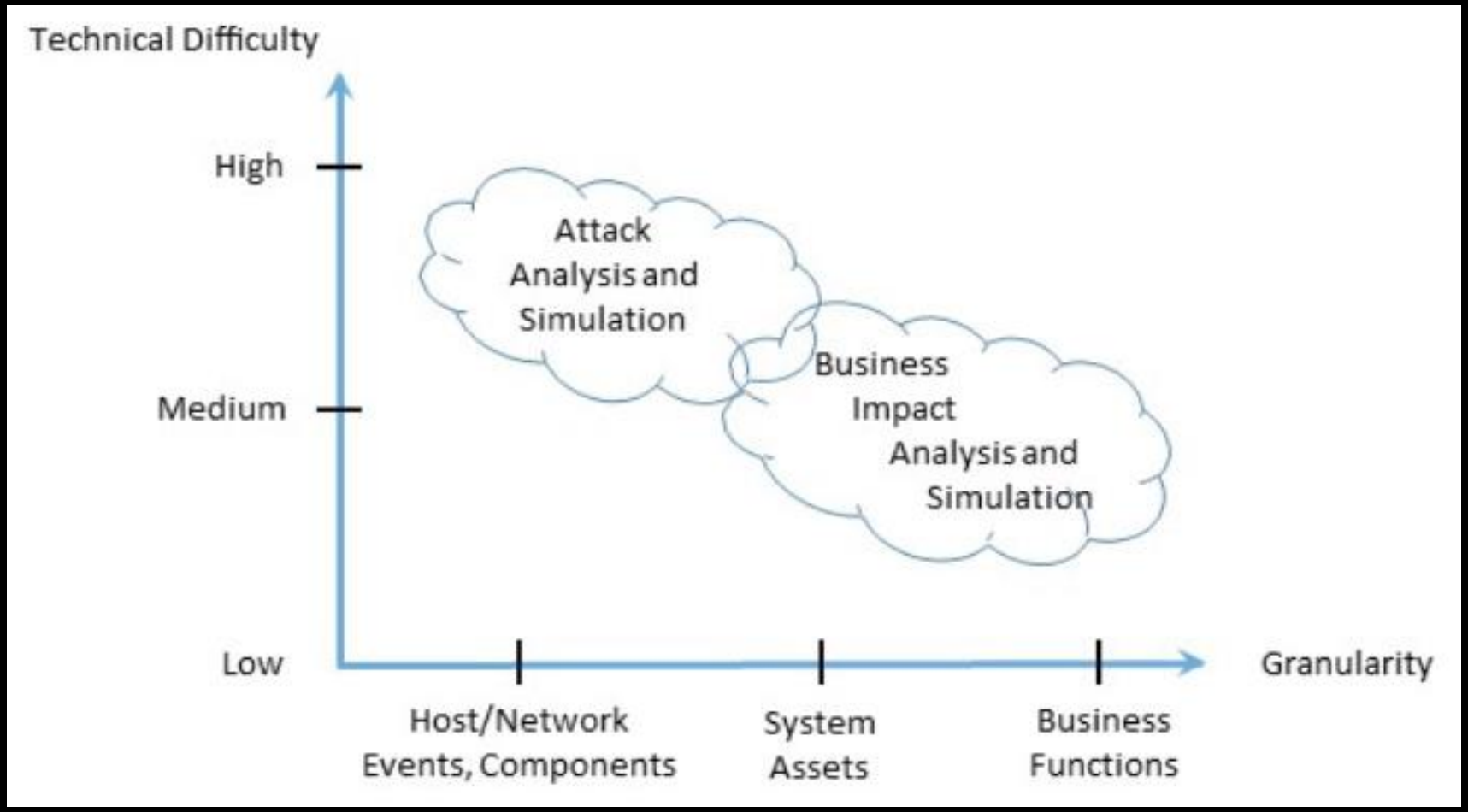
- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up



Cyber Mission Representation (DoD SBIR Conf – 2013)

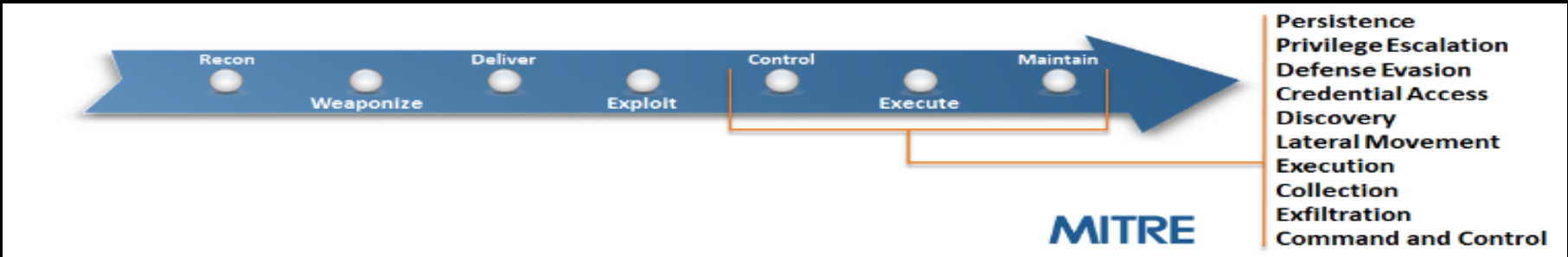
[1] https://www.dhs.gov/sites/default/files/publications/csd-sbir-2013-drsteven-king.pdf

Two major subspaces of cyber M&S problems



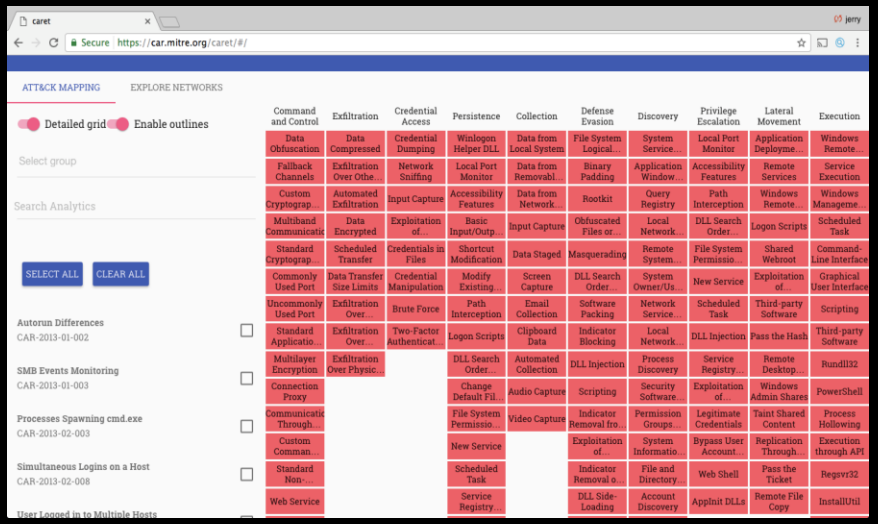
[1] NATO IST 094

MITRE & ATT@CK Framework[1]



- ATT@CK provides decomposition of cyber attack cycle

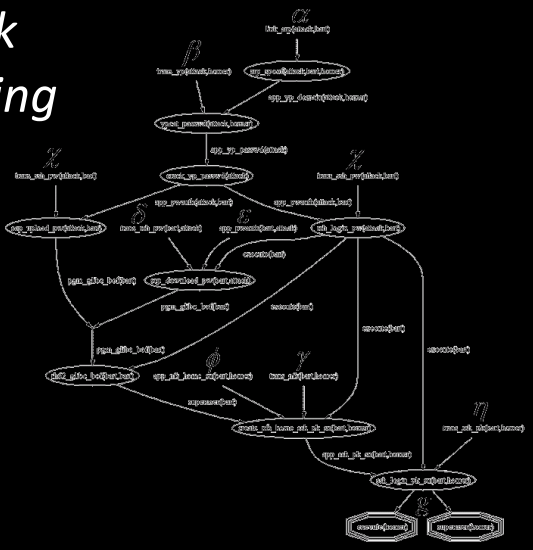
- CARET[2] expands ATT@CK to give more context on tactics, tools and threat groups



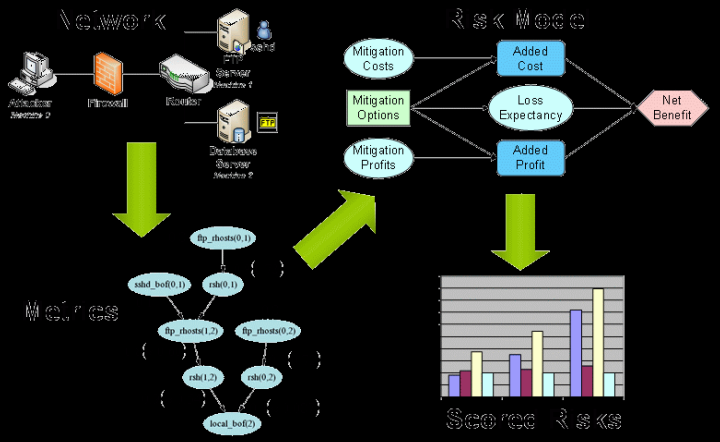
[1] https://attack.mitre.org/wiki/Main_Page
[2] https://car.mitre.org/caret/#/

Cauldron

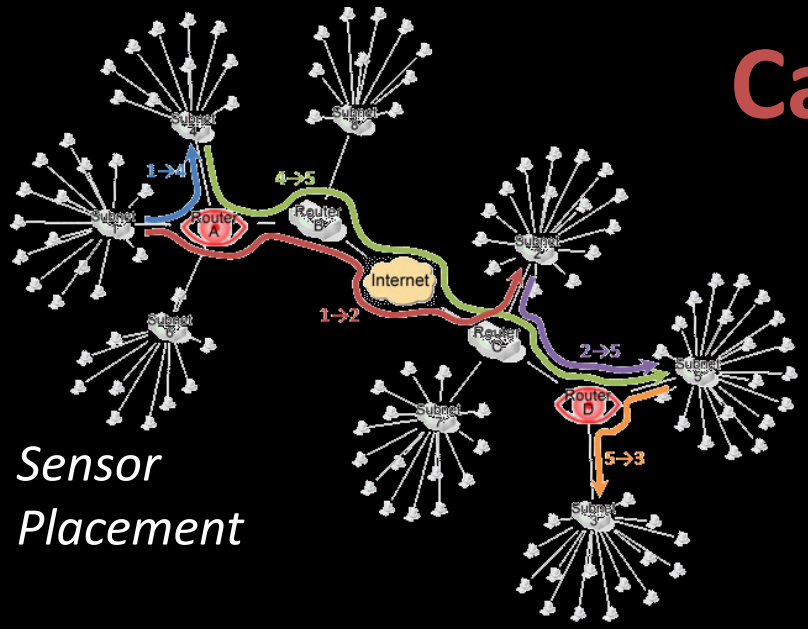
Network Hardening



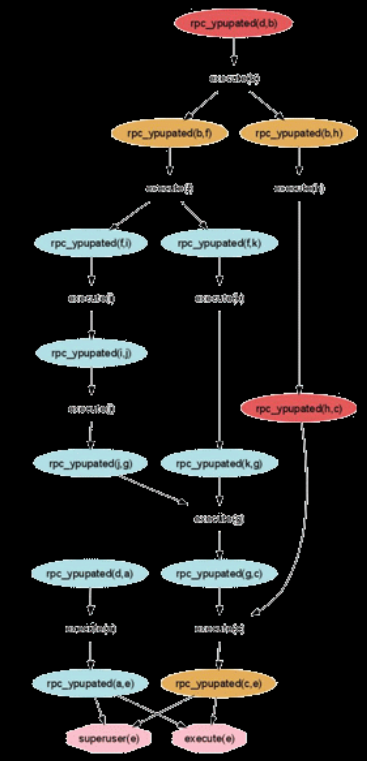
Security Metrics



Sensor Placement



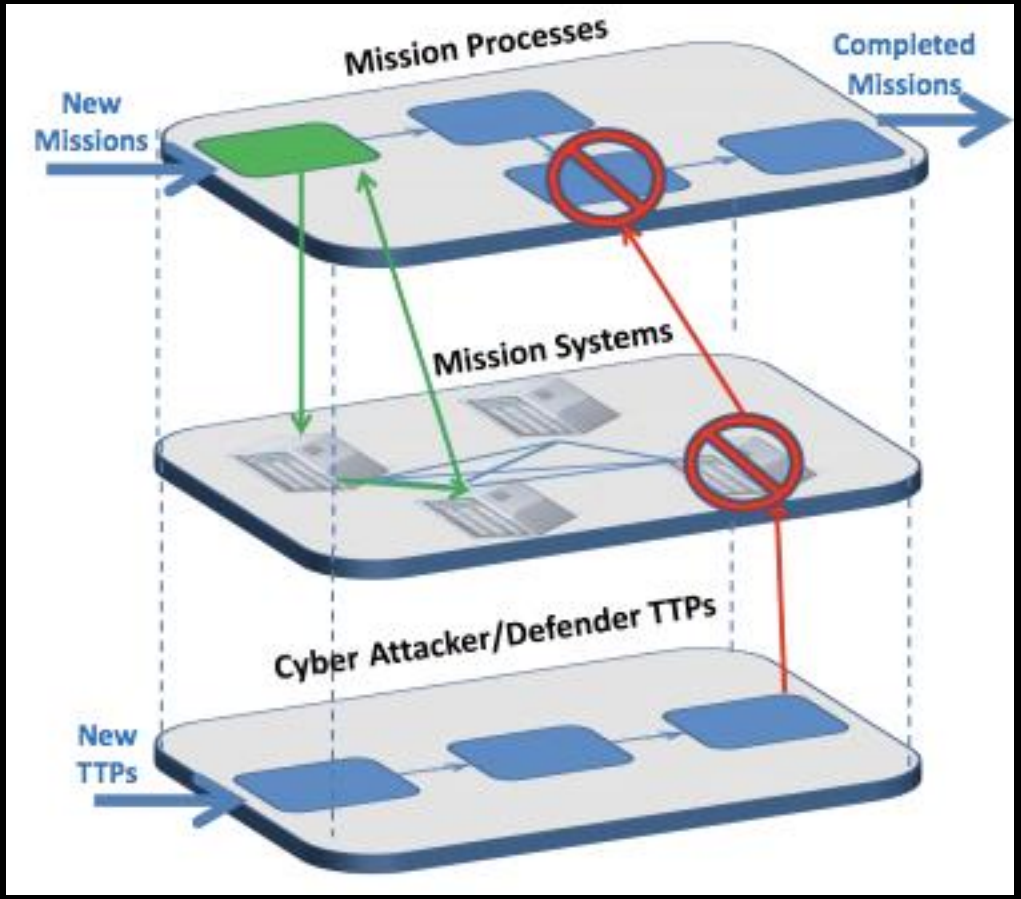
Alarm Correlation And Attack Response



Analyzing Mission Impacts of Cyber Actions (AMICA)[1][2]

For mission analysts, we seek to answer mission impact questions

For cyber defenders and analysts, we consider security posture



[1] 2015 NATO IST 128 Workshop (https://pdfs.semanticscholar.org/ff89/1d6348e2e2f01b3eef52126b45c64110a0a1.pdf)
[2] http://csis.gmu.edu/noel/pubs/2015_AMICA.pdf

Contents

- Science of Cyber Security
- Developing Communities
- Cyber Risk Evaluation & Assessment
- Cyber Model Example
- Current Evaluations
- Developing Work
- Wrap Up

Wrap Up

Cyber Threads	Examples
People	• Mission Operators • Cyber Security Professionals • M&S Professionals that help design secure cyber systems
Process	• Insurance Evaluation • Assessment Frameworks • Knowledge Based Design • Range Testing • Modeling Process for Developing Secure Cyber Systems
Technology	• Attack / Dependency Graphs • Layered Network Simulators • Threat Frameworks